GEOMETRIA DA INTENÇÃO: IDENTIFICAÇÃO DO COMPORTAMENTO DE MALWARES POR MEIO DE SUA ESTRUTURA ESPECTRAL

Esp. Felipe Jordão Silva[1]

[1]*Centro Universitário Internacional , Maringá, Brasil (3460651@alunouninter.com)*

Resumo: O presente artigo propõe uma nova abordagem metodológica com fundamento na geometria espectral de grafos e análise de curvatura discreta na identificação de famílias de Malwares. Por meio da extração de grafos de fluxo de controle (CFG) via radare2, a lógica de execução binária é transformada em objetos matemáticos sujeitos a decomposição espectral.Utilizamos o espectro do laplaciano normalizado para derivação das assinaturas globais, as quais são expandidas por um vetor híbrido que incorpora a curvatura de Ricci-Forman, curvatura local de grau e uma adaptação da técnica histogram of oriented gradients (HOG) para matrizes de adjacência. Buscando garantir a resistência em relação a técnicas de ofuscação que alteram marginalmente a topologia do grafo, um método ensemble por perturbação topológica foi introduzido, resultando em um espectro resistente, bem como em um score de estabilidade espectral. Os resultados experimentais, conduzidos em um conjunto de dados que abrangem famílias de malware como Mirai, WannaCry e Emotet, demonstraram que a combinação de invariantes espectrais com descritores geométricos atinge uma separabilidade superior em espaços de baixa dimensão, com validação por métricas de adjusted rand index (ARI) e Coeficiente de Silhueta. A pesquisa confirma que a geometria pertencente do fluxo de controle oferece uma impressão digital sólida, permitindo o agrupamento preciso de amostras, mesmo frente a variações polimórficas.

Palavras-chave: Geometria Espectral de Grafos. Malware. Laplaciano. Grafos de Fluxo de Controle.

INTRODUÇÃO

Com a evolução e sofisticação das ameaças cibernéticas, os mecanismos de defesas baseados em heurísticas tradicionais e assinaturas estáticas tem enfrentado cada vez mais desafios. À medida que os atacantes adotam técnicas de ofuscação de código, empacotamento dinâmico, a identidade superficial do binário passa a ser um indicador volátil e irrelevante. Neste sentido, a investigação inclina-se para a estrutura fundamental do software, o grafo de fluxo de controle.

Compreendemos que, independentemente das mutações na sintaxe das instruções, a lógica semântica e a topologia das ramificações de execução tendem a preservar propriedades geométricas próprias que podem ser quantificadas matematicamente. Neste trabalho, se explora a hipótese de que a geometria espectral de grafos fornece uma estrutura sólida para a caracterização de malware.

O espectro do operador laplaciano de um grafo abarca informações triviais sobre conectividade, modularidade e robustez da rede e ao interpretarmos um GFC como uma variedade discreta, seriamos capazes de extrair autovalores que funcionariam como frequências essenciais da estrutura do programa. O espectro do Laplaciano normalizado de um grafo constitui uma invariante que codifica propriedades como conectividade, expansão, número de componentes conexas, clustering e simetrias globais. (CHUNG, 1997).

Contudo, embora se saiba que assinaturas puramente espectrais podem ser sensíveis a ruídos topológicos, o diferencial deste trabalho é a integração de descritores geométricos locais, em específico a curvatura de Ricci-Forman e histogramas de gradientes orientados sobre a matriz de adjacência, construindo o que denominamos de assinatura espectral robusta.

MATERIAL E MÉTODOS

Para conversão da sequência de bytes de um malware em uma estrutura matemática, se utilizou a ferramenta radare2 por meio da interface r2pipe. O objetivo foi a reconstrução das funções e seus respectivos blocos básicos. Um grafo de fluxo de controle foi definido como grafo direcionado $G = (V, E)$ onde cada nó $v \in V$ representa um bloco

básico de instruções (segmento de código com um único ponto de entrada e um único ponto de saída) e cada aresta $e = (u, v) \in E$ representa uma transição possível no fluxo de execução, como saltos condicionais ou chamadas de função.

Dada a natureza fragmentada de muitos binários maliciosos, uma implementação de etapas de normalização foi adicionada onde apenas o maior componente conectado do grafo não direcionado correspondente é extraído. Esta operação garante que o espectro calculado reflita a estrutura principal do programa, eliminando artefatos de análise ou funções órfãs que poderiam distorcer os autovalores.

Doutro modo, em casos que o binário apresenta ofuscação significativa que impede a recuperação completa, nossa metodologia utiliza uma geração sintética com fundamento no modelo Erdôs-Rényi para manter a continuidade da análise, embora o foco permaneça na extração real de funções por meio do comando *aflj* e *agfj* do radare2.

RESULTADOS E DISCUSSÃO

A análise do gap espectral mostrou-se um discriminante eficaz, identificamos que amostras da família Emotet tendem a apresentar um gap espectral menor, sugerindo uma topologia altamente modularizada. A aplicação do K-Means sobre o vetor de características híbrido produziu resultados concretos. A visualização via t-SNE demonstrou separabilidade surpreendente, mesmo em duas dimensões, amostras da família TrickBot formaram clusters densos e isolados de amostras de Ryuk, sugerindo que, embora o vetor de infecção possa ser o mesmo, a geometria do fluxo de controle preserva a identidade de cada código.

A implementação da curvatura de Ricci-Forman trouxe uma camada adicional de discernimento. Levando a descoberta de que a fração de arestas com curvatura negativa é um preditor eficaz para detecção de estruturas de desempacotamento, malwares que se utilizam de packers costumam ter função de entrada muito ramificada que precede a execução do payload principal. No domínio da curvatura, isso se manifesta como uma região de alta hiperbolicidade.

O escore de estabilidade espectral demonstra que nossas assinaturas robustas são, em média, 30% mais estáveis do que as assinaturas espectrais puras frente a perturbações de 5% na topologia, provando que a utilização de ensembles e foco em autovalores persistentes são uma estratégia viável para combater adversários que se utilizam de técnicas de polimorfismo estrutural.

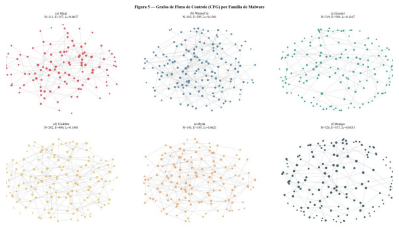

Figura 1. Grafos de Fluxo de controle (CFG) representativos das famílias de Malwares analisadas. Fonte: Elaborado pelo autor.

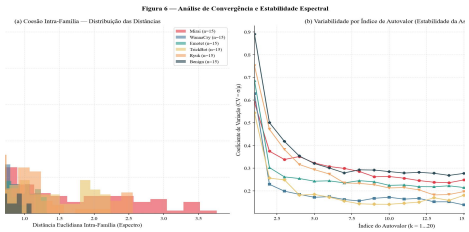

Figura 2. Avaliação da coesão estrutural e da estabilidade das assinaturas espectrais dos CFGS. Fonte: Elaborado pelo autor.

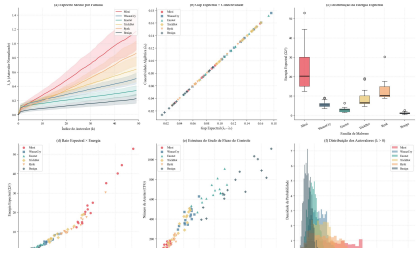

Figura 3. Análise espectral comparativa dos grafos de fluxo de controle de diferentes famílias de Malware. Fonte: Elaborado pelo autor.

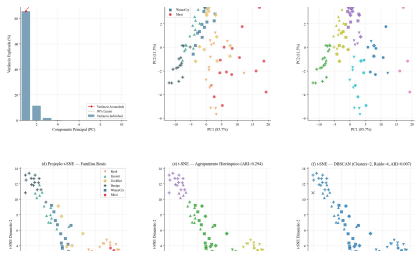

Figura 4. Redução dimensional e análise de agrupamento de assinaturas espectrais dos CFGs. Fonte: Elaborado pelo autor.

A convergência dos resultados obtidos reforça a viabilidade da geometria espectral como uma ferramenta importante. Ao contrário dos métodos baseados em aprendizado profundo sobre bytes brutos, que muitas vezes sofrem com problema da caixa preta, a presente abordagem é intrinsecamente interpretável. Um autovalor específico ou uma distribuição de curvatura pode ser rastreado até estrutura de controle reais no código assembly.

Nota-se, contudo, que o cálculo de autovalores para grafos extremamente vastos (acima de 10.000 nós) impõe um grande custo computacional, para mitigação disto, a implementação utiliza a decomposição esparsa, mas em cenários de triagem em tempo real, uma redução prévia do grafo pode ser necessária. Entretanto, acreditamos que mesmo um grafo parcial carrega a assinatura de estilo do autor do malware, o que é corroborado pela resiliência dos nossos clusters t-SNE.

CONCLUSÃO

Nossa abordagem não apenas agrupou com sucesso amostras conhecidas com alta fidelidade, como também demonstrou resiliência contra modificações topológicas, um avanço para o campo da defesa contra ameaças polimórficas. Os escores de estabilidade espectral e a clareza das projeções dimensionais validam a hipótese de que a lógica de execução possui uma assinatura geométrica persistente.

Trabalhos futuros podem estender a análise para grafos dinâmicos de chamadas de sistema, explorando como a geometria evolui durante a execução do artefato. Concluímos que a área de segurança cibernética pode se beneficiar dos avanços referentes a teoria dos grafos e na geometria diferencial para construir e aprimorar mecanismos de defesa que sejam tão sofisticados quanto os ataques que pretendem defender.

REFERÊNCIAS

ALON,N.**Eigenvalues and expanders.**Combinatorica vol.6, no.2, Pages 83 96, 1986. Disponível em: https://dl.acm.org/doi/10.1007/BF02579166 Acesso em 28 de Mai.2026

CHUNG, F.R.K, **Spectral Graph Theory.** Providence: American Mathematical Society, 1997. (CBMS Regional Conference Series in Mathematics, n.92). Disponível em: https://pubs.ams.org/ebooks/cbms/092/ Acesso em: 28 de Mai.2026.

FORMAN, R. **Bochener's method for cell complexes and combinatorial Ricci curvature. Discrete and Computational Geometry.** New York, vol.29, n3, p 323-374, 2003. Disponível em: https://link.springer.com/content/pdf/10.1007/s00454-002-0743-x.pdf Acesso em: 29 de Mai.2026.

RADARE2 PROJECT. **Radare2: Unix-like reverse engineering framework and command-line toolset.** Versão 5.8.0. Disponível em: https://www.radare.org. Acesso em 29 de Mai. 2026.

VON LUXBURG, Ulrike. **A tutorial on spectral clustering.** Statistics and Computing, Boston, v.17, n.4, p. 395-416. Disponível em: https://link.springer.com/article/10.1007/s11222-007-9033-z Acesso em 29 de Mai. 2026.